ІНФОРМАЦІЙНА БЕЗПЕКА ЯК ПІДСИСТЕМА В СИСТЕМІ ЕКОНОМІЧНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА

***Іванова В.В.**, магістр, Харківський національний університет міського господарства імені О. М. Бекетова*

Об'єктивно категорія інформаційна безпека виникла з появою засобів інформаційних комунікацій між людьми, а також з усвідомленням людиною наявності у людей і їх співтовариств інтересів, яким може бути завданий збитку шляхом дії на засоби інформаційних комунікацій, наявність і розвиток яких забезпечує інформаційний обмін між всіма елементами соціуму.

На сучасному етапі еволюції методів управління в організаціях все чіткіше постає питання інформаційної безпеки, як найголовнішого інструменту провадження ефективної діяльності компанії. Інформаційна безпека підприємства впливає на всі аспекти життєдіяльності організації, а також невід'ємно пов'язана з її економічною безпекою. А економічна безпека підприємства являє собою достатньо широке поняття - це і фінансова, і силова, і технико-технологічна, і кадрова, і правова, і інформаційна безпеки.

Інформаційна безпека сьогодні є одним з найважливіших чинників, що забезпечує існування та розвиток інформаційного середовища бізнесу. Чому сьогодні величезні інвестиції спрямовуються у той напрямок, який ще 5 років тому вважався безперспективним? Чому сьогодні керівники реагують на запрошення обговорити тематику інформаційної безпеки значно швидше, ніж на можливість обговорення стратегії підвищення ефективності управління компанією? Чому подальший розвиток бізнесу та суспільства неможливий без забезпечення цілісності інформаційного поля?

Відповіді на ці та інші питання привели автора статті до думки вивчити роль, визначити місце і рівень впливу інформаційної безпеки як складової у загальній системі економічної безпеки організації.

Інформаційна безпека (англ. Information Security) — стан інформації, в якому забезпечується збереження визначених політикою безпеки властивостей інформації.

Поняття інформаційна безпека у вітчизняній літературі багатозначно. Єдиного підходу до визначення цієї категорії в загальному сенсі ще не вироблено. Слід зазначити, що поняття «інформаційна безпека» розглядали Бондаренко В.О., Литвиненко О.В., Кормич Б.А., Остроухов В.В., Стрельцов А.А., Расторгуев С.П., Баринов А., Бучило И.Л. та ін., але, на наш погляд, інформаційна безпека – це стан його інформаційної захищеності, за якої спеціальні інформаційні операції, акти зовнішньої інформаційної агресії та негласного зняття інформації (за допомогою спеціальних технічних засобів), інформаційний тероризм і комп'ютерні злочини не завдають суттєвої шкоди інтересам підприємства.

В Україні інформаційна безпека здійснюється шляхом захисту інформації — у випадку, коли необхідність захисту інформації визначена законодавством в галузі захисту інформації. Для реалізації захисту інформації створюється Комплексна система захисту інформації (КСЗІ). Або, у випадку, коли суб'єкт інформаційної безпеки має наміри розробити і реалізувати політику інформаційної безпеки і може реалізовувати їх без порушення вимог законодавства:

- міжнародними стандартами ISO: ISO/IEC 17799:2005, ISO/IEC 27001:2005 та ін. — для підтримки рішень на основі ITIL та COBIT і виконання вимог англ. Sarbanes-Oxley Act (акту Сербайнза-Оклі про відповідальність акціонерів за обізнаність про стан своїх активів). Тоді на підприємстві створюється Система управління інформаційною безпекою (СУІБ), яка повинна відповідати усім вимогам міжнародних стандартів в галузі інформаційної безпеки.
- власними розробками.

Інформаційна безпека підприємства - це комплекс організаційних та технічних заходів, що забезпечують виконання чи вирішення питань захисту інформації. Бізнес починає оперувати не матеріальними, а інформаційними ресурсами. Зараз головна цінність бізнесу - це не матеріальні активи, а інформаційний здобуток компанії. Наприклад, інформація щодо клієнтів компанії, інформація щодо постачальників якісного продукту, інформація про фінансові, матеріальні взаємодії з компаніями, іншими бізнес-струкутрами. Цей список можна продовжувати, але важливість та цінність інформації сьогодні є очевидною. Ми маємо багато прикладів, один з яких могли б навести: пригадаймо атаку на інформаційні бази інвестиційної компанії в США та втрата інформації щодо персональних рахунків і карткової інформації клієнтів призвели до судових позовів та подальшого поглинання компанії, яка була знецінена конкурентами.

Можна поставити питання про те, що інформаційна безпека є лише механізмом для забезпечення життєдіяльності підприємства, тобто вона навряд чи дає що-небудь для розвитку та руху бізнесу вперед.

Давайте порівняємо інформаційну безпеку з безпекою автомобіля. Уявіть собі, що ви вибираєте автомобіль. Питання захисту пасажира, водія, забезпечення захисту дітей зазвичай стоїть на другому місці після параметрів місткості. Подушки безпеки, посилена рама, ABS, інші елементи безпеки не впливають на ходові якості автомобіля, проте вони є абсолютно критичними в складних ситуаціях для забезпечення вашого здоров'я і захисту Вашого життя. Абсолютно аналогічно інформаційна безпека є чинником виживання компанії в жорсткому конкурентному середовищі, до того ж надає право і шанс водієві на дуже щільній трасі рухатися з більшою швидкістю, чим інші учасники бізнес-руху, не боячись за наслідки.

Часто, не дивлячись на оптимістичні прогнози, стійкий і динамічний розвиток бізнесу, через декілька років підприємство виявляється перед загрозою банкрутства, виникає необхідність додаткового фінансування. Вважається, що до таких втрат приводить незадовільне керівництво, слабка

кадрова політика і відсутність достатнього досвіду в цій сфері діяльності. Проте більш глибше вивчення ситуації, показує, що насправді використовується витончена схема шахрайства і розкрадання фінансових коштів через порушення існуючих норм інформаційної безпеки організації.

Які ж є критерії безпеки інформації компанії? Коли можна сказати, що компанія захищена? Які є засоби захисту?

Проведемо ще одну аналогію тепер вже між інформаційною безпекою і здоров'ям людини. Ви можете вважати себе здоровим, Вас можуть не турбувати неприємні відчуття, проблеми, але об'єктивну оцінку Вашого здоров'я зможе дати тільки професіонал - лікар, який зможе на основі свого досвіду, відомих методик, Вашого аналізу сказати наскільки Ви здорові, на що варто звернути увагу, і з чим треба почати боротися. Аналогічно відбувається і в інформаційній безпеці. Тільки діагностика називається аудитом, діагнози - ті ураження, якими може бути підвернена Ваша інформаційна система, а ліки і здоровий спосіб життя - це ті засоби захисту, які пропонуються Вам для нейтралізації знайдених загроз. Як і в лікарській практиці, так і в практиці інформаційного аудиту, існує зовнішній огляд (аудит) і інструментальні дослідження – внутрішній аналіз безпеки.

Засоби захисту можна розділити на три основні категорії:

1. Ті продукти безпеки, які дозволяють Вам вирішити гостру насущну проблему, - «зняти головний біль» (ліки);

2. Ті довготриваючі процеси безпеки, які дозволять Вам побудувати правильну політику безпеки, що знижує проблеми інформаційної безпеки в довготривалій перспективі, яка знижує ризик безпеки довгострокових перспектив («правильний спосіб життя», профілактика захворювань).

3.Цілісність інформаційного поля.

На будь-якому підприємстві необхідно створити цілісність і впорядкованість інформаційного поля для забезпечення контролю та прозорості бізнесу. Інформаційне поле компанії, візуалізацією якого є IT служба, по своїй суті є віддзеркаленням основного бізнесу. В умовах економіки, яка швидко розвивається, інтенсивності інвестицій і бізнес-підходів, що постійно змінюються, чітке розуміння того, що відбувається в компанії, можливе лише при налагодженій системі інформаційного забезпечення бізнесу, тому що інформаційне поле - це дзеркало будь-якого підприємства.

Будь-яка безпека потребує інвестицій. Інфомаційна безпека бізнесу потребує «розумних» інвестицій. Інвестиції залежать від розуміння та можливих наслідків самої проблеми порушення інформаційних кордонів бізнесу. Виключно з цієї позиції можна аналізувати та прогнозувати власну інвестиційну політику. Виходячи з досвіду, можу сказати, що представники середнього та малого бізнесу завдяки жорсткій конкурентній боротьбі дуже гарно розуміються на проблемах інформаційної безпеки. Більшість з них інвестують власні кошти на підтримання недоторканості своєї комерційної інформації та інформації щодо своїх клієнтів і продуктів.

Ідеальної безпеки не існує, але продуманість організаційно-технічних заходів лежить в основі і правильної інвестиційної політики, і правильної технічної політики будь-якої організації.

Під інформаційною безпекою підприємства зазвичай розуміють стан найбільш ефективного використання корпоративних ресурсів для запобігання погрозам і забезпеченню стабільного функціонування компанії. Подальший розвиток управлінської думки в Україні, очевидно, повинен принести усвідомлення ключової ролі аналітичної складової менеджменту, тобто функції забезпечення менеджерів актуальною, спеціально орієнтованою на ухвалення рішень інформацією про внутрішнє і зовнішнє середовище фірми.

Управління безпекою, зокрема інформаційною, повинно знаходиться у веденні департаменту IT. В той же час, у веденні департаменту безпеки повинні знаходиться люди, які мають право тотального контролю реалізацій політик безпеки, і, зокрема, на рівні відділу IT. Тобто, ми розділяємо виконавчу і контрольну функції між департаментом IT і департаментом безпеки відповідно. Керівник департаменту IT і керівник департаменту безпеки мають бути членами ради директорів, і брати безпосередню участь не лише в реалізації, але і у формуванні бізнес-стратегії компанії.

Українські компанії зараз знаходяться на дуже важливій стадії переходу до безпаперового електронного діловодства і електронного способу ведення бізнесу. Саме такі компанії повинні звертати увагу на питання інформаційної безпеки. Концентрація великих об'ємів інформації в інформаційній системі потенційно може привести до зловживання при обробці цієї інформації, і лише правильно поставлені процеси інформаційної безпеки і комплексний підхід до рішення завдань безпеки дозволить надійно і гарантовано захистити інформацію на усіх етапах її обробки, зокрема персональної інформації.

Давайте поглянемо на 7 років назад. Скільки мобільних телефонів було у вас, ваших знайомих? Зараз більшість людей мають мобільний телефон, навіть більше одного. Зараз наша залежність від інформаційного поля, в якому ми живемо і комунікуємо, значно зросла. Сьогодні порушення цього поля буде впливати не тільки на компанії, корпорації, організації - його проблеми стають проблемами кожного з нас. Ми є повністю залежними від інформаційного оточення та інструментів комунікацій з соціумом. Тому життєздатність інформаційного оточення, працездатність інструментів є чи не основним фактором існування соціуму. Виходячи з цього, особливо важливим питанням є забезпечення безпеки та надійності функціонування всіх цих механізмів, про які вище сказано. Той, хто володіє інформацією - володіє світом. Той, хто не володіє - втратив його на віки. Сьогодні інформація вирішує все. Але щоб «володіти світом», треба свою інформацію захищати.